ROLE-BASED ACCESS IN A MULTI-CUSTOMER COMPUTING ENVIRONMENT

FIELD OF THE INVENTION

[0001] The present invention relates to role-based access in multi-customer distributed and/or centralized computing environments.

BACKGROUND

[0002] Corporate employees and customers need access to systems resources and applications in secure and reliable environments. The administration and control of access to such resources is made more challenging with the growing trend toward corporate employee and customer turnover, the use of temporary contract personnel as a core supplement to a corporation's workforce, the continuous installation of new applications, as well as updates to and the removal of existing applications from corporate networks. Security administration has become an increasingly more complex and expensive aspect of the management of large enterprise networks given these trends.

[0003] Role-based access control ("RBAC") technologies and methods have evolved from the research and development efforts of the United States Department of Defense, as well as David Ferraiolo and Richard Kuhn, among others, in response to the growing challenge of security administration. Role-based access control has emerged as one of the accepted models for security administration in large, networked computing environments. RBAC technology is being developed and deployed in areas such as defense, health care, as well as banking and finance.

[0004] Role-based access control entails the categorization of computer system users into roles. A role is, for example, a construct that is created by a systems administrator according to, for example, the job functions performed by users within an organization. Computer system users can be assigned to roles on the basis of their particular job responsibilities and qualifications. Users are not assigned access permissions directly. Instead, roles are granted various permissions or access authorizations to data and/or systems resources based on the authority and responsibility conferred upon users that are assigned to these roles. Roles allow for an additional level of abstraction that facilitates security administration at the enterprise-level rather than at the user-level, in part, because the mapping of roles to permissions is more stable than the mapping of users to roles. The latter mapping changes each time a user is added or removed from the system, changes job functions, or is promoted. These changes are more frequent than those in the role-to-permission mapping. Role-to-permission mapping is typically driven by changes in business policies. Such business policies typically change less frequently than changes to the job functions of users. Thus, the use of role-based access control models can simplify the task of administering authorization and permission policies. There are, however, limits to this simplification. In large computing environments, the number of roles may be in the thousands. Management of these large number of roles and maintenance of user-role mappings can be arduous, expensive, and time-consuming.

[0005] More rigorous RBAC models have been introduced that employ, for example, role hierarchies where roles can inherit permissions from other roles. RBAC models that involve the imposition of restrictions on policy and access configurations also exist. One of the more common restrictions or constraints is represented by mutually exclusive roles, where the same user can be assigned to only one role among a mutually exclusive group of one or more roles. There are RBAC models that employ the notion of prerequisite roles where a user may only be assigned to role "A" if he is already assigned to role "B."

[0006] Though these more rigorous RBAC models provide an adaptive means of enforcing security policies at the enterprise-level, the extent to which such models have allowed for reduced complexity, increased scalability, and true flexibility in the process of security administration has been limited. Defining roles and permissions sufficiently and assigning appropriate user-role associations within an enterprise with a heterogeneous IT infrastructure continues to be extremely complex and costly. The application of role-based access control models to administer user entitlements across multiple applications and computing environments remains a challenge.

SUMMARY OF THE INVENTION

[0007] In one aspect, there is a method for managing role-based access in a multi-customer computing environment. An actor is associated with a role, a policy type is associated with the role, and a role scope is associated with the role. One or more values are received for one or more corresponding context parameters associated with the actor. A request for access to a resource is received from the actor. A policy instance is determined based on the policy type and the one or more values for the one or more corresponding context parameters associated with the actor. One or more actor-role scope values are determined based on the role scope and the one or more values for the one or more corresponding context parameters associated with the actor. A response to the request is determined based on the policy instance and the actor-role scope values.

[0008] In other examples, one or more of the following features can be included. In response to the request a resolved scope can be determined using the actor-role scope values. A role assignment record can be generated. The role assignment record can include the actor, the role, and/or the context parameters. The role assignment record can include the one or more actor-role scope values based on the role scope. The resource can include a database, a system application, a document, or any combination thereof. The actor can include a user, a system account, a system application, a computing device, or any combination thereof. The policy type can include an access control policy element, a data view/presentation policy element, a function performance/update operation policy element, or any combination thereof. Determining the policy instance can include employing a hierarchical priority of the one or more of the context parameters. A default policy instance can be defined. The default policy instance can be selected when there is no match with the one or more of the context parameters.

[0009] In another aspect, there is a system for managing role-based access in a multi-customer computing environment. The system can include one or more servers configured to perform any of the methods described herein. In another aspect, there is a computer program product, tangibly embodied in an information carrier, for managing role-based access in a multi-customer computing environment.